TNI TOTAL NETWORKS INC. | JOIN THE FAMILY!

Job Title: Security Engineer

Security Operations Engineering Tasks

- Ensure compliance with security policies, develop and update IT security documentation, provide related status reports, briefings, schedules, and project plans in written form.
- Plan and implement security reviews for changes impacting hardware, software, baselines, connections, or applications.
- Collaborate with staff to plan and implement new firewall architectures, upgrades and features as necessary.
- Assist in the administration of all firewalls to include updates, upgrades, policy administration, and validation.
- Perform other security related tasks, including vulnerability scanning and log management.
- Assist in reviewing and implementing customer changes consistent with existing policies.
- Review and update documentation to ensure consistency with current procedures.
- Manage and tune additional software blades associated with firewall architecture (IPS, URL, Application Control, AV, Advanced Malware detection).
- Follow industry best practices, NIST SP 800-53, and agency security policy standards to identify gaps and inefficiencies in the security infrastructure and provide options for resolving them.
- Make recommendations to modernize the client’s security infrastructure in a more effective and efficient manner.
- Explain new security requirements to client staff and contractors to support implementation.
- Work outside of normal business hours to support outage resolution, planned maintenance, or to implement an upgrade.
- Perform other related duties.

QUALIFICATIONS

- Eight (8) years of experience in Information Technology, Cybersecurity, or a related field.
- Minimum six (6) years of experience configuring and administering firewall technologies such as carrier class Checkpoint Firewalls, Palo Alto and Network Security Policy Management.
- In-depth knowledge of security operations, including firewall rules and security policies.
- Strong networking ability and knowledge of firewall platforms to assist in rapid identification and isolation of issues during incidents and outages.
- Experience working with RMF and NIST SP 800-53 (Rev 4/5).
- Expert knowledge of RMF accreditation packages and all steps of the RMF process.
- Knowledge of cyber-attack patterns, tactics, techniques, and procedures.
- Ability to adapt security processes/tools to evolving landscapes and risk scenarios.

- Strong knowledge of Checkpoint firewall hardware modifications.
- Strong knowledge of iBoss Cloud IPS and IDS configurations.
- Strong knowledge of SSLV Symantec security application.
- Ability to work both independently and within a team environment.
- Ability to work in a fast-paced environment while maintaining outstanding customer service skills.
- Proficiency in explaining complex policies and protocols in simple terms.

PREFERRED EDUCATION:

Bachelor's degree in an IT related field Preferred

CERTIFICATIONS:

CCSE, CISSP, CISM, Security+, CASP

SECURITY CLEARANCE:

Top Secret security clearance.